IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Japanese Patent Application NO.: 2004-007683
Filing Date: January 15, 2004
For: APPARATUS INCLUDING UNIT FOR VERIFYING APPARATUS-SPECIFIC INFORMATION AND METHOD OF VERIFYING APPARATUS-SPECIFIC INFORMATION

VERIFICATION OF TRANSLATION

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Yoshio SHIOHARA residing at c/o NII Patent Firm, located at 6F, Tanaka Ito Pia Shin-Osaka Bldg., 3-10, Nishi Nakajima 5-chome, Yodogawa-ku, Osaka-city, Osaka 532-0011, Japan declares:

(1) that he knows well both the Japanese and English languages;
(2) that he translated APPARATUS INCLUDING UNIT FOR VERIFYING APPARATUS-SPECIFIC INFORMATION AND METHOD OF VERIFYING APPARATUS-SPECIFIC INFORMATION from Japanese to English;
(3) that the attached English translation is a true and correct translation of APPARATUS INCLUDING UNIT FOR VERIFYING APPARATUS-SPECIFIC INFORMATION AND METHOD OF VERIFYING APPARATUS-SPECIFIC INFORMATION to the best of his knowledge and belief; and
(4) that all statements made of his own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such false statements may jeopardize the validity of the application or any patent thereon.

This 15th day of September, 2010

Yoshio Shiohara

Yoshio SHIOHARA

[Document] Patent Application
[Our Reference Number] 2048150075
[Submission Date] January 15, 2004
[Direction] Commissioner, Patent Office
[International Patent Classification] G09C 1/00
[Inventor]
[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006 Oaza Kadoma, Kadoma-Shi, Osaka
[Name] Kaoru Yokota
[Inventor]
[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006 Oaza Kadoma, Kadoma-Shi, Osaka
[Name] Motoji Ohmori
[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006 Oaza Kadoma, Kadoma-Shi, Osaka
[Name] Koichi Morioka
[Inventor]
[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006 Oaza Kadoma, Kadoma-Shi, Osaka
[Name] Hideshi Ishihara
[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006 Oaza Kadoma, Kadoma-Shi, Osaka
[Name] Makoto Tatebayashi
[Applicant]
[Identification Number] 000005821

[Name] MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd.

[Patent Attorney]

[Identification Number] 100097445

[Name] Fumio Iwahashi

[Selected Patent Attorney]

[Identification Number] 100103355

[Name] Tomoyasu Sakaguchi

[Selected Patent Attorney]

[Identification Number] 100109667

[Name] Hiroki Naito

[Indication of Fee]

[Prepayment Registration Number] 011305

[Filing Fee] ¥21,000

[List of Enclosures]

[Document] Claims 1

[Document] Specification 1

[Document] Drawings 1

[Document] Abstract of the Disclosure 1

[Power of Attorney Reference Number] 9809938

[Document] Claims

[Claim 1]

A method of verifying secret information stored in an apparatus and specific to the apparatus, said method comprising:

transmitting, to the apparatus, an instruction for outputting index information attached to the secret information specific to the apparatus; and

outputting the index information stored in the apparatus in response to the instruction.

[Claim 2]

An apparatus having a function of verifying secret information which is stored in said apparatus and specific to said apparatus, said apparatus comprising:

a reception unit configured to receive an instruction command for verifying the secret information specific to said apparatus, the instruction command being transmitted from outside said apparatus;

an index information storage unit configured to store index information which is attached to the secret information specific to said apparatus and uniquely indicates the secret information specific to said apparatus;

a secret information storage unit configured to store the secret information specific to said apparatus in such a manner that the secret information is not accessible from outside said apparatus; and

an output unit configured to output, to outside said apparatus, the index information stored in said index information storage unit, when said reception unit receives the instruction command.

[Claim 3]

An apparatus having a function of verifying secret information which is stored in said apparatus and specific to said apparatus, said apparatus comprising:

a reception unit configured to receive an instruction command for verifying the secret information specific to said apparatus, the instruction command being transmitted from outside said apparatus;

an index information storage unit configured to store index information which is attached to the secret information specific to said

apparatus and uniquely indicates the secret information specific to said apparatus;

an encryption unit configured to encrypt the index information;

a secret information storage unit configured to store the secret information specific to said apparatus in such a manner that the secret information is not accessible from outside said apparatus; and

an output unit configured to output, to outside said apparatus, the index information stored in said index information storage unit and encrypted by said encryption unit, when said reception unit receives the instruction command.

[Claim 4]

The apparatus according to Claim 2 or Claim 3,

wherein the index information includes identification data for identifying the secret information specific to said apparatus and verification data resulting from a predetermined conversion of the identification data.

[Claim 5]

The apparatus according to any one of Claim 2 to Claim 4,

further comprising a recording medium mount unit into which a recording medium is externally loaded,

wherein, when a recording medium on which a program including the instruction command is recorded is loaded into said recording medium mount unit, said reception unit is configured to receive the instruction command included in the program recorded on the recording medium.

[Claim 6]

The apparatus according to any one of Claim 2 to Claim 4,

wherein said reception unit is a communication terminal.

[Claim 7]

The apparatus according to any one of Claim 2 to Claim 4,

wherein said reception unit is a terminal for debugging used in development of said apparatus.

[Claim 8]

The apparatus according to Claim 5,

wherein a unique identification number is recorded on the recording medium, and

said reception unit includes an instruction execution permission unit configured to check whether or not the identification number of the recoding unit loaded into said recording medium mount unit satisfies a predetermined condition and receive the instruction command only when the condition is satisfied.

[Claim 9]

An apparatus having a function of verifying secret information which is stored in said apparatus and specific to said apparatus, said apparatus comprising

an index information display unit configured to display index information which is attached to the secret information specific to said apparatus and uniquely indicates the secret information specific to said apparatus.

[Claim 10]

An apparatus having a function of verifying secret information which is stored in said apparatus and specific to said apparatus, said apparatus comprising

an index information display unit configured to display either index information which is attached to the secret information specific to said apparatus or encrypted index information resulting from encrypting the index information.

[Document] Specification

[Title of the Invention]

APPARATUS INCLUDING UNIT FOR VERIFYING APPARATUS-SPECIFIC INFORMATION AND METHOD OF VERIFYING APPARATUS-SPECIFIC INFORMATION

[Detailed Description of Invention]

[0001]

[Technical Field]

The present invention relates to apparatuses having a unit for verifying information specific to each of the apparatuses and embedded therein, and methods of verifying information specific to each of the apparatuses.

[0002]

[Related Art]

In a digital content copyright protection method for recording media including optical discs, such as a Digital Versatile Disc (DVD), and a semiconductor recording media, such as a Secure Digital (SD) memory card and a memory stick, content data recorded in the media is encrypted. The encrypted content data is decrypted for reproduction using a key embedded in a reproduction apparatus. Under a license from a licensor for use of the copyright protection method, a manufacturer of the reproduction apparatus is provided with a key necessary for decryption of the content data (hereafter referred to as a device key) along with a license for manufacturing the reproduction apparatus. The license agreement includes security implementation specifications (compliance rules, robustness rules). Under the license agreement, the licensed manufacturer are ordered to implement the received device key in the reproduction apparatus in a manner such that a certain level of security standard is satisfied and to output content data in plaintext resulting from decryption performed in the reproduction apparatus to outside the reproduction apparatus via a general external interface, but not to output the content data to an user-accessible bus in the reproduction apparatus. Such mechanism of the content encryption using a device key and compliance with the implementation specifications under an

agreement may prevent the content recorded on the media from being illegally copied to a recording medium such as a hard disk or illegally distributed to the Internet.

[0003]

However, such mechanism alone cannot resist the threat caused in the case where the protection implemented when the manufacturer embedded the device key in the reproduction apparatus is disabled and the device key is exposed. In other words, a user who has analyzed and exposed the device key may use the device key so as to generate and distribute an unauthorized copying tool which allows decryption of the encrypted content data and copying the content data on a hard disk (that is, a tool in violation of the security implementation specifications). However, the content encryption mechanism alone cannot prevent such inappropriate actions by the analyzer.

[0004]

Key revocation techniques have therefore been employed in many copyright protection methods as countermeasures against such exposure of device keys. Specifically, there is a method of key revocation disclosed in Non-Patent Reference 1, for example. In this key revocation method, reproduction apparatuses are each provided with a device key unique to each of the reproduction apparatus. In addition, each device key is assigned index information which identifies the device key (hereafter referred to as device key index information). The device key index information is provided to each of the reproduction apparatuses along with the corresponding device key. The reproduction apparatus decrypts the encrypted content data using the device key and the device key index information attached to the device key. This key revocation technique allows revocation of an exposed device key, so that content data to be written in a recording medium manufactured after the revocation or content data recorded on the recording media manufactured after the revocation cannot be decrypted using the revoked device key. Details about the technique are disclosed in Non-Patent Reference 1, and thus further explanation thereof is not provided here. In the key revocation technique, unique

device keys are thus embedded in reproduction apparatuses so that exposed device keys can be individually revoked.

Non-Patent Reference 1: Seiji Okuaki, Bagus Santoso, Kazuo Ohta, "Hybrid System of Complete Subtree and Subset Difference Method", Proceedings of Symposium on Cryptography and Information Security, Volume I, pp. 221–226, 2003

[Problems that Invention is to Solve]

[0005]

In the key revocation technique, manufactures are required to embed a unique device key in each reproduction apparatus in a manner such that the device key cannot be externally read, in accordance with conditions of the agreement. This is very inconvenient for the manufacturers of the reproduction apparatus. Because, in the case where there is a request from an end user for repair of a malfunctioning reproduction apparatus, the manufacturer needs to know details of the device key embedded in the reproduction apparatus in order to locate a malfunction, particularly to determine whether or not the malfunction is in a decryption processing unit. For example, under a circumstance where some device keys have actually been revoked, it is necessary to know details of the device key in order to determine whether the reproduction apparatus to be repaired is a reproduction apparatus in which one of the revoked device keys is embedded.

[0006]

On the other hand, the following problem is also found when viewed from another perspective. It is necessary to use a device key unique to each reproduction apparatus. On the other hand, a licensor of the copyright protection method needs to be allowed to verify as necessary whether or not the manufacturer of the reproduction apparatus, which is a licensee, is neglecting the license agreement and committing a fraud such as embedding the same device keys in reproduction apparatuses. Although there is such a necessity, identifying embedded device keys is presently very difficult because device keys are implemented in a manner such that reading device keys embedded in the reproduction apparatuses is not allowed.

[0007]

The present invention, conceived to address the problem, has an object of providing a method of verifying apparatus specific-information which identifies keys embedded in apparatuses even in the case where the keys are implemented in the apparatuses in a manner such that the keys cannot be externally read.

[Means to Solve the Problems]

[0008]

In order to address the problem with the conventional technique, the apparatus having a unit for verifying secret information which is stored in the apparatus and specific to the apparatus includes: a reception unit configured to receive an instruction command for verifying the secret information specific to the apparatus, the instruction command being transmitted from outside the apparatus; an index information storage unit configured to store index information which is attached to the secret information specific to the apparatus and uniquely indicates the secret information specific to the apparatus; and an output unit configured to output, to outside the apparatus, the index information stored in the index information storage unit, when the reception unit receives the instruction command.

[0009]

With this configuration, the apparatus according to the present invention allows identification of secret information specific to apparatuses even after the apparatus is shipped as a product.

[Effects of the Invention]

[0010]

The method of verifying apparatus-specific information by the present invention allows verification of an apparatus-specific device key embedded in the apparatus even after the device key is implemented in a manner such that the device key cannot be externally read.

[Embodiments of the Present Invention]

[0011]

Hereinafter, an embodiment according to the present invention

is described with reference to figures.

[0012]

Exemplary Configurations 1 to 4 below each allow verification of a device key in an apparatus 1 according to the present embodiment.

[First Embodiment]

[0013]

(Exemplary Configuration 1)

FIG. 1 shows Exemplary Configuration 1 which allows verification of a device key embedded in the apparatus 1 using a method of verifying apparatus-specific information according to the present invention.

[0014]

Exemplary Configuration 1 includes the apparatus 1, an optical disc 2, and a display apparatus 3. In the apparatus 1, a device key specific to the apparatus 1 and device key index information attached to the device key are embedded. In the optical disc 2, a program to display details of the device key embedded in the apparatus on the display apparatus 3 is stored. On the display apparatus 3, the video data provided from the apparatus 1 is displayed. The apparatus 1 and the display apparatus 3 each have an interface for video input and output. The optical disc 2 may be a DVD, a Blu-day disc (BD), or a CD. The apparatus 2 may be a DVD player, a DVD recorder, a BD recorder. The video input and output interface may be an RGB terminal, an RCA video terminal, an S-Video terminal, or a D-terminal. The apparatus 1 and the display apparatus 3 are connected through a connection cable corresponding to any one of these terminals.

[0015]

A method of obtaining information on the device key embedded in the apparatus 1 is as follows. First, the optical disc 2 is loaded into the apparatus 1. Next, the apparatus 1 reads the program recorded on the optical disc 2 and outputs the device key index information according to the program. The device key index information output from the apparatus 1 is provided to the display apparatus 3 through the connection cable. The display apparatus 3 displays on the screen an image indicating the device key index information. The index

information indicates the embedded device key. Operation of the apparatus 1 from the loading of the optical disc 2 to the outputting of the device key index information is detailed later. In Exemplary Configuration 1, the apparatus 1 already includes an optical disc read unit and the video output interface, and therefore additionally required to the apparatus 1 is only a program to output the device key index information. Therefore, the new function can be added at a small cost.

[0016]

(Exemplary Configuration 2)

According to the present embodiment, information of the device key can be obtained not only by Exemplary Configuration 1 but also by Exemplary Configuration 2.

[0017]

FIG. 2 shows Exemplary Configuration 2 which allows verification of a device key embedded in the apparatus 1 using a method of verifying apparatus-specific information according to the present invention.

[0018]

Exemplary Configuration 2 includes the apparatus 1 as with Exemplary Configuration 1, a debug apparatus 41, a display apparatus 42, and an input apparatus 43. The debug apparatus 41 is an apparatus for debugging programs such as a program in the apparatus 1. The display apparatus 42 displays data received from the debug apparatus 41. The input apparatus 43 provides input made by an operator of the debug apparatus 41 to the debug apparatus 41. The debug apparatus 41 is the same one as a debug apparatus used in development of the apparatus 1. The apparatus 1 and the debug apparatus 41 each have a debug terminal such as a Joint Test Action Group (JTAG) terminal. These terminals are connected through a connection cable, such as a JTAG cable, which is compliant with terminals for connecting debug apparatuses. Furthermore, the debug apparatus 41 and the display apparatus 42 are connected through a connection cable compliant with the debug terminal used with the debug apparatus 41. So are the debug apparatus 41 and the

input apparatus 43.

[0019]

A method of obtaining information on the device key embedded in the apparatus 1 is as follows. First, the debug apparatus 41 connected to the apparatus 1 is started. Next, the operator inputs an instruction for displaying the device key index information in the apparatus 1 into the debug apparatus 41 using the input apparatus 43. In response to the instruction, the debug apparatus 41 transmits a predetermined instruction code to the apparatus to cause the apparatus 1 to output the device key index information. In response to the instruction code, the apparatus 1 transmits the device key index information stored in the apparatus 1 to the debug apparatus 41. Next, the debug apparatus 41 converts the received device key index information into a data in a format displayable on the screen of the display apparatus 42, and then transmits the data to the display apparatus 42. The display apparatus 42 displays the device key index information on the screen using the data received. Operation of the apparatus 1 from the receiving of the instruction code to the transmitting of the device key index information to the debug apparatus 41 is detailed later.

[0020]

In Exemplary Configuration 2, the interface for debugging used in development of the apparatus is directly used. Advantageously, there is thus no need for a dedicated interface for obtaining the device key index information. Furthermore, because an interface for debugging is necessary, general users who does not have debbugger terminals or debug environments for development of the apparatus are prevented from improperly browsing the device key index information.

[0021]

(Exemplary Configuration 3)

According to the present embodiment, information of the device key can be obtained also by Exemplary Configuration 3 described below.

[0022]

FIG. 3 shows Exemplary Configuration 3 which allows verification of a device key embedded in the apparatus 1 using a method of verifying apparatus-specific information according to the present invention.

[0023]

Exemplary Configuration 3 includes the apparatus 1 and the display apparatus 3 as with the Exemplary Configurations 1 and 2, a network 5, and a server 6. The network 5 is used for data transmission to and from the server 6. The server 6 transmits an instruction command to cause the apparatus 1 to output the device key information therein. The apparatus 1 has an interface for connection with the network 5. Specifically, the interface is a LAN terminal, for example.

[0024]

A method of obtaining information on the device key embedded in the apparatus 1 is as follows. First, an operator performs a predetermined operation on the apparatus 1 in order to cause the display apparatus 3 to display a maintenance menu. For example, a special switch which allows the operator to move to maintenance mode is provided on the apparatus 1. The operator presses the switch to move to maintenance mode. Next, the operator selects a menu item of "Execute process of obtaining device key index information". The operator may make this selection using a button provided on the apparatus 1 or a remote control attached to the apparatus 1. Upon the selection of the menu item, the apparatus 1 transmits a connection request to the server 6 via the network 5. In response to this request, the server 6 verifies whether or not the operator 1 is an authorized person to perform the process which the operator is requesting (that is, displaying the device key information) by password authentication. Specifically, user names and passwords of authorized operators are registered on the server in advance, and the server 6 authorizes an operator when the operator correctly enters the registered user name and password. When the operator is thus authorized, the server 6 transmits, via the network 5, an instruction command to cause the apparatus 1 to output the device key

information to the apparatus 1. In response to the instruction command, the apparatus 1 provides the device key index information to the display apparatus 3, and then the display apparatus 3 displays the information on the screen. Operation of the apparatus 1 from the receiving of the instruction command to the providing of the device key index information to the display apparatus 3 is detailed later.

[0025]

According to Exemplary Configuration 3, there is an advantageous effect that apparatuses, such as a DVD recorder, which have a communication interface for update of EPG information or programmed recording via the network do not need any dedicated interface to receive device key index information.

[0026]

Furthermore, by the verification of operators as to whether or not they are authorized to view the device index key, the server 6 prevents the device index key being viewed by unauthorized operators.

[0027]

(Exemplary Configuration 4)

According to the present embodiment, information of the device key can be obtained also by Exemplary Configuration 4.

[0028]

FIG. 4 shows Exemplary Configuration 4 which allows verification of a device key embedded in the apparatus 1 using a method of verifying apparatus-specific information according to the present invention.

[0029]

Exemplary Configuration 4 includes the apparatus as with Exemplary Configurations 1, 2, and 3, a network 5, a display terminal 72, and an input terminal 73. The network 5 is used for data transmission to and from a computer terminal 71. The display terminal 72 displays information provided from the computer terminal 71. The input terminal 73 is used for inputting data into the computer terminal 71. The apparatus 1 and the computer terminal 71 each have an interface for connection with the network 5.

Specifically, the interface is a LAN terminal, for example. On the computer terminal 71, a program is installed which monitors device key information embedded in the apparatus 1.

[0030]

A method of obtaining information on the device key embedded in the apparatus 1 is as follows. First, the program which monitors the device key is started on the computer terminal 71 to which the apparatus 1 is connected via the network 5. Next, an operator of the computer terminal 71 inputs, using the input terminal 73, an instruction for displaying the device key index information into the computer terminal 71. In response to the instruction, the computer terminal 71 transmits, to the apparatus 1 via the network 5, an instruction code which causes the apparatus 1 to output the device key index information. In response to the instruction code, the apparatus 1 transmits the device key index information to the computer terminal 71. Next, the computer terminal 71 converts the received device key index information into a data in a format displayable on the screen, and then transmits the data to the display terminal 72. Based on the data received, the display apparatus 72 displays the device key index information of the apparatus 1 on the screen. Operation of the apparatus 1 from the receiving of the instruction code from the computer terminal 71 to the transmitting of the device key index information to the computer terminal 71 is detailed later.

[0031]

According to Exemplary Configuration 4, there is an advantageous effect that apparatuses, such as a DVD recorder, which have a communication interface for update of EPG information or programmed recording via the network do not need any dedicated interface to receive device key index information.

[0032]

(Internal Configuration and Operation of Apparatus 1)

FIG. 5 is a block diagram showing an internal configuration of the apparatus 1 according to the present embodiment.

[0033]

The apparatus 1 includes a main processing unit 10, a video processing unit 11, a video output unit 12, a debug external I/F 13, a communication I/F 14, a disc read unit 15, an cryptographic processing unit 17, a RAM 18, a device ID storage unit 19, a device key storage unit 110, a program storage unit 111, and a data bus 16. The main processing unit 10 controls other processing units, input and output through interfaces, and read and write of the storage units. The video processing unit 11 converts data internally processed in the apparatus 1 into a data format displayable on the display apparatus 3. The video output unit 12 outputs the data to be displayed to the display apparatus 3. The debug external I/F is an input and output interface to exchange data with the debug apparatus 41. The communication I/F 14 is a communication interface to connect to an external network such as a LAN. The disc read unit 15 reads and writes data on the optical disc loaded in the apparatus 1. The cryptographic processing unit 17 performs encryption necessary for reproduction of content data. The RAM 18 temporally stores a program or data which is processed in the apparatus. The device ID storage unit 19 stores the device key index information attached to the device key embedded in the apparatus 1. The device key storage unit 110 stores the device key. The program storage unit 111 stores the program to be executed in the apparatus 1. The data bus 16 transfers data among the modules. The video output unit 12 may be an RGB terminal, an RCA video terminal, an S terminal, a D terminal. The debug external I/F 13 may be a JTAG terminal. The communication I/F 13 may be a LAN terminal.

[0034]

The device key index information and the device key are encrypted using a certain encryption method such as the Data Encryption Standard (DES) and stored in the device ID storage unit 19 and the device key storage unit 110, respectively. The key used in the encrypting (master key) is stored in the cryptographic processing unit 17 in a manner such that the master key cannot be externally read. In the program storage unit 111, programs for processes to be performed in the apparatus 1 are stored. The programs stored in the

program storage unit 111 include a program which describes a process of output of the device key index information in response to an external instruction command. Data of these programs is compressed and recorded in the program recording unit 111. The compressed data is decompressed when the apparatus 1 is turned on, and then transferred to the RAM 18.

[0035]

Hereinafter, processes performed in the apparatus 1 are described for respective cases of Exemplary Configurations 1 to 5.

[0036]

(Case of Exemplary Configuration 1)

A process of output of the device key index information by the apparatus 1 is hereinafter described with reference to FIG. 1 and FIG. 5.

[0037]

When the optical disc 2 in which the program for displaying the device key index information is stored is inserted into the disc slot of the apparatus 1, the disc read unit 15 reads data of the program written on the optical disc 2. The read program data is transferred to the main processing unit 10 via the data bus 16. The main processing unit 10 reads a command for outputting the device key index information included in the program data, and performs the following process according to the program which is stored in the RAM 18 and in which the process of outputting of the device key index information is described.

[0038]

First, the main processing unit 10 reads encrypted device index information stored in the device ID storage unit 19 and sends it to the cryptographic processing unit 17. The cryptographic processing unit 17 decrypts the encrypted device index information. The decrypted device index information is converted by the video processing unit 11 into a data format displayable on the image display apparatus 3, and the converted data is output to the display apparatus 3 via the video output unit 12.

[0039]

(Case of Exemplary Configuration 2)

A process of output of the device key index information by the apparatus 1 is hereinafter described with reference to FIG. 2 and FIG. 5.

[0040]

A command for displaying the device key index information is input into the main processing unit 10 via the debug external I/F 13 and the data bus 16. In response to the command, the main processing unit 10 calculates decrypted device key index information by performing the same process as in Exemplary Configuration 1 according to the program in which the process of outputting of the device key index information recorded in the RAM 18 is described. The main processing unit 10 then outputs the resultant decrypted device key index information to the debug apparatus 41 via the debug external I/F 13.

[0041]

(Case of Exemplary Configuration 3)

A process of output of the device key index information by the apparatus 1 is hereinafter described with reference to FIG. 3 and FIG. 5.

[0042]

A command for displaying the device key index information is input into the main processing unit 10 via the communication I/F 14 and the data bus 16. In response to the command, the main processing unit 10 calculates decrypted device key index information by performing the same process as in Exemplary Configurations 1 and 2 according to the program in which the process of outputting of the device key index information recorded in the RAM 18 is described. The decrypted device index information is converted by the video processing unit 11 into a data format displayable on the image display apparatus 3, and the converted data is output to the display apparatus 3 via the video output unit 12.

[0043]

(Case of Exemplary Configuration 4)

A process of output of the device key index information by the

apparatus 1 is hereinafter described with reference to FIG. 4 and FIG. 5.

[0044]

A command for displaying the device key index information is input into the main processing unit 10 via the communication I/F 14 and the data bus 16. In response to the command, the main processing unit 10 calculates decrypted device key index information by performing the same process as in Exemplary Configuration 1 according to the program in which the process of output of the device key index information recorded in the RAM 18 is described. The resultant decrypted device key information is output, via the communication I/F 14, to the computer terminal 71 on which the program for monitoring information of the device key is installed.

[0045]

Although the device index information stored in the device key storage unit 110 is encrypted in the present embodiment, the device key index information may be stored without being encrypted. In this case, data read out of the device key storage unit 110 may be directly output as the device key index information.

[0046]

Furthermore, although the encrypted device key index information is first decrypted by the cryptographic processing unit 17 and then output in the present embodiment, the encrypted device key index information may be output as it is. In this case, a key to decrypting the encrypted device key index information is not stored in the cryptographic processing unit 17. It is possible that a key to decryption is stored in the apparatus which receives the data from the apparatus 1 in order to obtain device key index information by decrypting the encrypted device key index information, or that the encrypted device key index information is displayed without being encrypted. It is also possible that the device key index information decrypted by the cryptographic processing unit 17 is displayed after being further encrypted using another key. Furthermore, a key to decrypting the encrypted device key index information may be secretly held by a manufacturer of each apparatus so that nobody but

the manufacturer knows the device key index information. The device key index information is thus known only to the manufacturer of the apparatus.

[0047]

Furthermore, although the optical disc is loaded in the apparatus 1 in Exemplary Configuration 1 according to the present embodiment, a semiconductor recording medium, such as an SD memory card or a memory stick, or an IC card may be loaded instead.

[0048]

Furthermore, the following mechanism may be added to Exemplary Configuration 1 of the present embodiment in order to prevent general users from creating an optical disc in which an own-made program for displaying the device key information and browsing the device key index information in the apparatus is stored. First, an ID unique to each optical disc is written in a ROM area of the disc when it is manufactured. For example, an ID is written in a burst cutting area (BCA) of a DVD. Then, the instruction code for displaying the device key index information is executed by the apparatus only when a disc having a specific ID is inserted. The optical disc having the specific ID is not available to general users but only to the development manufacturer of the apparatus as a disc for maintenance. Consequently, even if a general user creates a program for displaying the device key index information, the general user, who cannot obtain the disc for maintenance, is not allowed to browse the device key index information in the apparatus.

[0049]

Although all of the Exemplary Configurations 1 to 4 are employed in the present embodiment, the apparatus or the method may be configured to include only one of them.

[0050]

In order for a licensor of the copyright protection method to check whether or not a licensee, that is, a manufacturer of apparatuses properly embeds unique device keys in respective apparatuses in the case where any one of the configurations of the present invention is applied, the licensor may force the licensee to

implement the command for outputting device key index information described above in the apparatuses by agreement. However, there is still the following problem. The problem is that the command is actually implemented but the device key index information output by the command is improperly changed to the one different the embedded device key index information. Specifically, although the identical device keys and identical device key index information are embedded in different apparatuses, it is still possible to make the licensor believe that the embedded device keys are unique by configuring the apparatuses to output false device key index information in response to the command. This malpractice can be prevented in the following manner. Defining the device key index information as DI, check information P = F(DI) is obtained by performing a secret conversion F which only the licensor knows. For F, for example, a cryptographic process of a secret key cryptographic method in which a key is secret to all but the licensor can be used. The licensor provides the licensee, the manufacturer of apparatuses, with the check information P in addition to the device key and the device key index information. On the other hand, the licensor forces the licensee by agreement to implement in the apparatus a command for displaying the device key index information and the check information in combination. With this configuration, the licensee, even if it creates false device key index information, cannot forge check information corresponding to the false device key index information. Therefore, such false device key index information output by the apparatus can be detected as forged device key index information by examining whether or not a pair of the device key index information DI and the check information P satisfies the relationship of P = F(DI). Furthermore, in eh case where the conversion F is also disclosed to the licensee in this method, the licensor may provide, to the licensee, not only the device key but also data prepared by encrypting, using a secret key which only the licensor knows, the check information P or combined data of the device key information DI and the check information P, and force the licensee to configure the apparatus to output the encrypted data in addition to the device key

index information or to implement in the apparatus an command for outputting the encrypted data instead of the device key index information. In this case, the licensor verifies whether or not the device key index information is forged based on data obtained by decrypting, using the secret key of the licensor, the encrypted data output from the apparatus according to the command.

[0051]

Furthermore, the device key index information may be indicated in the following manner instead of being displayed on the display apparatus or the like. (b) of FIG. 6 shows the apparatus 1 shown in (a) of FIG. 6 with a cover removed. The apparatus 1 includes a chassis 1a, a substrate 1b, and a device key index information indication unit 1c. As shown in (c) of FIG. 6, the device key index information indication unit 1c shows a numeric value which indicates the device key index information in the apparatus 1 in hexadecimal notation. The numeric value may be printed directly on the device key index information indication unit 1c by a printing method such as laser printing or may be presented on a board on which the device key index information is printed and which is attached onto the device key index information indication unit 1c by vises, adhesives, welding, or any other adhesive method. A sticker on which the device key index information is printed is also possible. The presented information is specifically, for example, a hexadecimal value indicating the decryption information Iu disclosed in the Non-Patent Reference 1. The cover of the apparatus 1 may be attached with screws or vises having such a special shape that general users cannot remove the cover. Furthermore, a place where the index information is indicated is not limited to the mentioned place and may be anywhere unless it can be recognized as the index information of the apparatus 1.

[Industrial Applicability]

[0052]

The apparatus according to the present invention, which produces an advantageous effect that information on an apparatus-specific key embedded in the apparatus is made available

by an instruction command externally transmitted to the apparatus, is applicable to apparatuses which have a function of copyright protection and store secret information unique to each of the apparatuses.

[Brief Description of Drawings]

[0053]

FIG. 1 is a block diagram showing Exemplary Configuration 1 including an apparatus 1, an optical disc 2, and a display apparatus 3 according to the embodiment of the present invention.

FIG. 2 is a block diagram showing Exemplary Configuration 2 including the apparatus 1, a debug apparatus 41, and a display apparatus 42 according to the embodiment of the present invention.

FIG. 3 is a block diagram showing Exemplary Configuration 3 including the apparatus 1, a network 5, the display apparatus 3, and a server 6 according to the embodiment of the present invention.

FIG. 4 is a block diagram showing Exemplary Configuration 4 including the apparatus 1, the network 5, a computer terminal 71, a display terminal 72, and an input terminal 73 according to the embodiment of the present invention.

FIG. 5 is a block diagram showing an exemplary configuration of the apparatus 1 according to the embodiment of the present invention.

FIG. 6 is a block diagram showing an example of the apparatus 1 according to the embodiment of the present invention.

[Numerical References]

1	Apparatus
2	Optical disc
3, 42	Display unit
5	Network
6	Server
10	Main processing unit
11	Video processing unit
12	Video output unit
13	Debug external I/F
14	Communication I/F
15	Disc read unit

16	Data bus
17	Encryption processing unit
18	RAM
19	Device ID storage unit
41	Debug apparatus
43	Input apparatus
71	Computer terminal
72	Display terminal
73	Input terminal
110	Device key storage unit
111	Program storage unit

[Document] Abstract of the Disclosure

[Abstract]

[Object]

Verifying secret information which is specific to the apparatus and stored in an apparatus in a manner such that the information is not accessible from outside the apparatus.

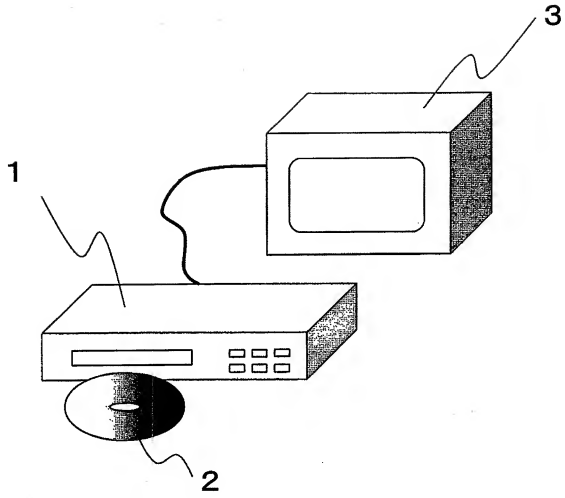
[Means to Achieve the Object]

The apparatus includes a reception unit, an index information storage unit, and an output unit. The reception unit receives an externally provided instruction command for verifying secret information specific to the apparatus. The index information storage unit stores index information attached to the secret information specific to the apparatus and uniquely indicating the secret information specific to the apparatus. The output unit outputs, to outside the apparatus, the index information stored in the index information storage unit when the reception unit receives the instruction command.

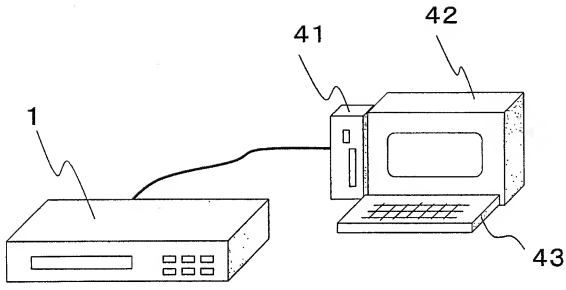
[Selected Drawing]Fig. 5

[Document] Drawings

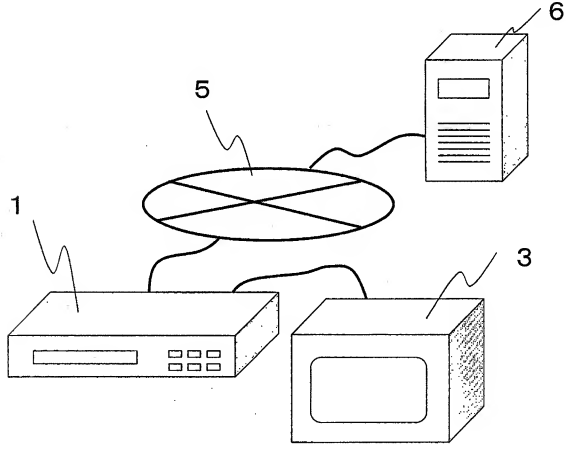
[FIG. 1]



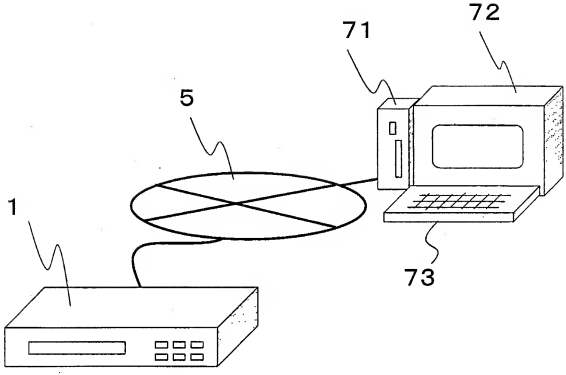
[FIG. 2]



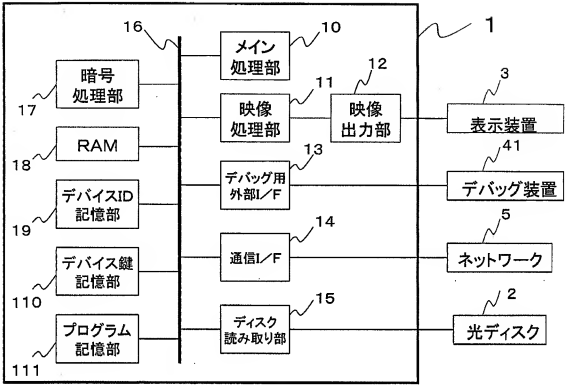
[FIG. 3]



[FIG. 4]



[FIG. 5]



2 Optical disc
3 Display unit
5 Network
10 Main processing unit
11 Video processing unit
12 Video output unit
13 Debug external I/F
14 Communication I/F
15 Disc read unit
17 Encryption processing unit
18 RAM
19 Device ID storage unit
41 Debug apparatus
110 Device key storage unit
111 Program storage unit

[FIG. 6]